Fermilab Authentication Policy for the General Computing Environment (GCE)

All computing services offered at Fermilab must require individuals to authenticate themselves by presenting a Laboratory-approved, trusted, reliable form of individual identification before making use of the service. The only exceptions to this policy are those services which Fermilab makes available to the general public, such as public web pages or accepting incoming email.

Approved authentication mechanisms of differing trustworthiness and complexity are provided by the Computing Sector. Which mechanism should be used for a particular computing service depends on the risks associated with potential use of the service by unauthorized or misidentified individuals, as specified below.

Use of approved authentication mechanisms is required for the following reasons:

- Fermilab is required to know who is using the Laboratory computing systems;
- Fermilab is required to be able to provide central disabling of individuals' accounts;
- Fermilab needs to be able to flexibly respond to changes in regulatory or threat environments;
- Authentication is most effectively implemented on a Laboratory-wide basis;
- A Laboratory-wide authentication service provides the basis for a role-based authorization platform.

Two groups of approved authentication mechanisms are provided. The first is required for services where there is a legal or enterprise need to maintain a high level of assurance of individual identity. Mechanisms in this group are automatically tied to the central lab identity management system. Thus, no credentials of this class can be issued for an identity which is disabled in the central system. Moreover, services that allow arbitrary program execution or general data transfer must use non-disclosing versions of authentication (which are designed to not require any authentication secrets to be transmitted over the network). Kerberos is an example of a non-disclosing mechanism.

The second group of approved authentication mechanisms is required for services where there is no legal or enterprise necessity for maintaining a high level of assurance of individual identity. Identities may be assigned through self registration. The underlying authentication mechanisms, as for DOE Grid certificates, may be managed external entities.

Password policy for the first type of services (which presently include Kerberos, Windows domain authentication, and Services domain authentication) is enforced by technical means, with complexity, revision and reuse requirements specified for each type of authentication (for example, LDAP Service Password Policy, DocDB ID 3108). Passwords for other services should use equivalent complexity policies, but these will be enforced through administrative means.

Individuals are only allowed to possess a single authentication account. Other credentials must be tied to the original account (for example, user/admin accounts are explicitly tied to the original user account.)